Security and Risk Management Strategies

In-Depth Research Overview

Windows Security Vista Appears More Promising

Version: 1.0, Jan 09, 2006

AUTHOR(S):

Dan Blum

(dblum@burtongroup.com)

TECHNOLOGY THREAD:

Perimeter and Infrastructure Security

Conclusion

Windows Server 2003 R2, Windows Vista, and Windows Server "Longhorn"—coupled with Microsoft's industry-level security initiatives, greater emphasis on secure development practices, and planned forays into content control—will bring many security enhancements forward over the next two years. None of these changes guarantees higher assurance in all cases, but in combination they do make the overall security picture for Microsoft's enterprise customers appear much more promising than it has been in recent years.

12130

Publishing Information

Burton Group is a research and consulting firm specializing in network and applications infrastructure technologies. Burton works to catalyze change and progress in the network computing industry through interaction with leading vendors and users. Publication headquarters, marketing, and sales offices are located at:

Burton Group
7050 Union Park Center, Suite 510
Midvale, Utah USA 84047-4169
Phone: +1.801.566.2880
Fax: +1.801.566.3611
Toll free in the USA: 800.824.9924
Internet: info@burtongroup.com; www.burtongroup.com

Burton Group's *Security and Risk Management Strategies* service provides objective analysis of networking technology, market trends, vendor strategies, and related products. The information in Burton Group's *Security and Risk Management Strategies* service is gathered from reliable sources and is prepared by experienced analysts, but it cannot be considered infallible. The opinions expressed are based on judgments made at the time, and are subject to change. Burton offers no warranty, either expressed or implied, on the information in Burton Group's *Security and Risk Management Strategies* service, and accepts no responsibility for errors resulting from its use.

If you do not have a license to Burton Group's *Security and Risk Management Strategies* service and are interested in receiving information about becoming a subscriber, please contact Burton Group.

Table Of Contents

Synopsis

Security will be a key issue for Microsoft's planned Windows Server 2003 Release 2 (R2), Windows Vista client, and Windows Server “Longhorn” releases. Although no one should categorically predict victory in advance for Windows security, many of the details recently released at the Professional Developers Conference (PDC) 2005 and other venues appear promising.

On the plus side, Microsoft rebuilt and reengineered the operating system (OS) code used in both client and server through improved development processes; embraced the principle of least privilege through User Account Control and other measures. Microsoft will also increase reliability by isolating some device drivers from the OS kernel and providing a more secure boot process (called BitLocker Drive Encryption) and full-volume encryption with Trusted Platform Module (TPM) support in Windows Vista. Microsoft will also make browser security improvements in Internet Explorer 7.0 (IE7), and ship authentication enhancements such as InfoCard, changes to the logon process, and support for federated identity.

Also important for customers whose Active Directory domain controllers hold the keys to the kingdom, enterprises will be able to deploy a stripped-down “Server Core” package that eliminates many OS features that are not necessary for domain controller operation.

On the minus side, there will not be a stripped-down, hardened client package, and ActiveX support in the browser will continue indefinitely, albeit with more security controls. The client OS attack space will still include something north of 60 million lines of code, and considerable complexity will result from the intricate processing required to provide least-privilege mode operation while remaining backward compatible to ActiveX and as many legacy applications as possible. Also, given its market share, Windows will remain the most popular target for attackers.

Risk and complexity notwithstanding, the world needs a general-purpose OS. Security isn't everything, and reasonable people can argue one way or the other about the tradeoffs that Microsoft has made. Once in the field, Windows Vista will also benefit from the substantial investments Microsoft has made in integrated content control offerings, incident response processes, user education, cooperation with law enforcement, and patch management update systems.

Analysis

At its Professional Developers Conference (PDC), Microsoft often raises the curtain on new or planned technologies. This year at PDC 2005 in Los Angeles was no exception, as Microsoft continued the process of clarifying plans for the Windows Vista client operating system (OS) release, unveiled plans for Office 12, shed some light on Windows server OS futures, and offered tantalizing hints of WinFS, an integrated relational file system.

Bill Gates began the PDC by saying Microsoft had originally wanted to make Windows “as secure and reliable as the electrical network.” He noted, however, that this statement was issued before the Los Angeles blackout descended on September 12, 2005. Today, he would amend it to “become as secure and reliable as the electrical network should be.” Both the electrical network and Windows have a long way to go, but in Windows' case at least, multiple improvements are underway.

Executives and demonstrators made a strong pitch to the audience that the Windows Vista Client and Office 12—which Microsoft says will ship together in the “second half of 2006”—will be worth the wait. Microsoft also released a raft of upgrades for Windows Server 2003 Release 2 (R2) at the end of 2005, and has more in store for the still-code-named “Server ‘Longhorn'” in 2007. Figure 1 diagrams Burton Group's understanding of Microsoft's road map for major releases and their features of interest.

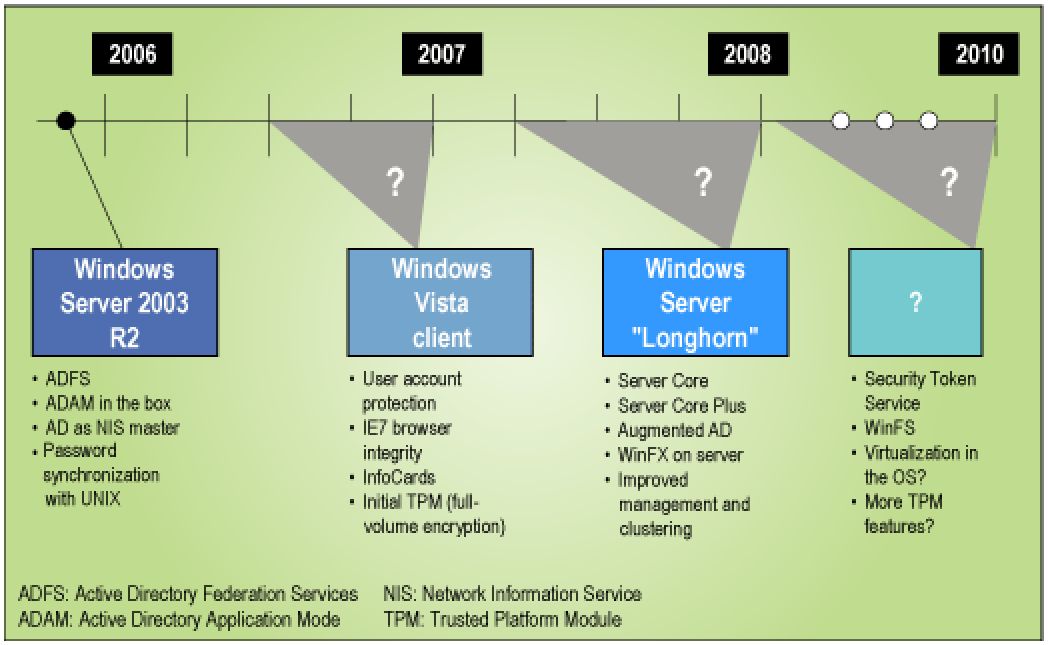
2006
2007
2008
2010
?
?
?
Windows Server 2003 R2
Windows Vista client
Windows Server "Longhorn"
?
• ADFS
• ADAM in the box
• AD as NIS master
• Password synchronization with UNIX
• User account protection
• IE7 browser integrity
• InfoCards
• Initial TPM (full-volume encryption)
• Server Core
• Server Core Plus
• Augmented AD
• WinFX on server
• Improved management and clustering
• Security Token Service
• WinFS
• Virtualization in the OS?
• More TPM features?
ADFS: Active Directory Federation Services
ADAM: Active Directory Application Mode
NIS: Network Information Service
TPM: Trusted Platform Module

Figure 1: *Microsoft Release Road Map*

Microsoft is laboring to create a smooth transition for developers and customers to a new operating system environment. There will be security improvements, but risks will remain in the increased complexity of new behaviors that seek to balance security, compatibility with older applications, and user convenience. Also, while there is no doubt now that the plethora of new features in Windows Vista, Office 12, R2, and Server “Longhorn” will add considerable value, it remains to be seen whether this value creates compelling reasons for enterprise customers to march rapidly toward new deployment.

New OS Names and High-Level Architecture

As its end of 2006 release date draws closer, the client OS once known as Longhorn and all its components now have official names, consigning the likes of “Avalon” and “Indigo” to the realm of nostalgia.

The graphical user interface called “Avalon” has been renamed to the Windows Presentation Foundation (WPF), and the web services programming environment once known as “Indigo” is now dubbed the “Windows Communication Foundation” (WCF). WPF and WCF sit alongside the “Windows Data Foundation” (WDF). Collectively, WCF, WPF, and WDF constitute “WinFX,” which runs over the .NET Framework 2.0 interface to the “base OS.” Please accept our apologies for the many acronyms, and examine Figure 2 for a better perspective on how the pieces of Windows Vista fit together at a high level.

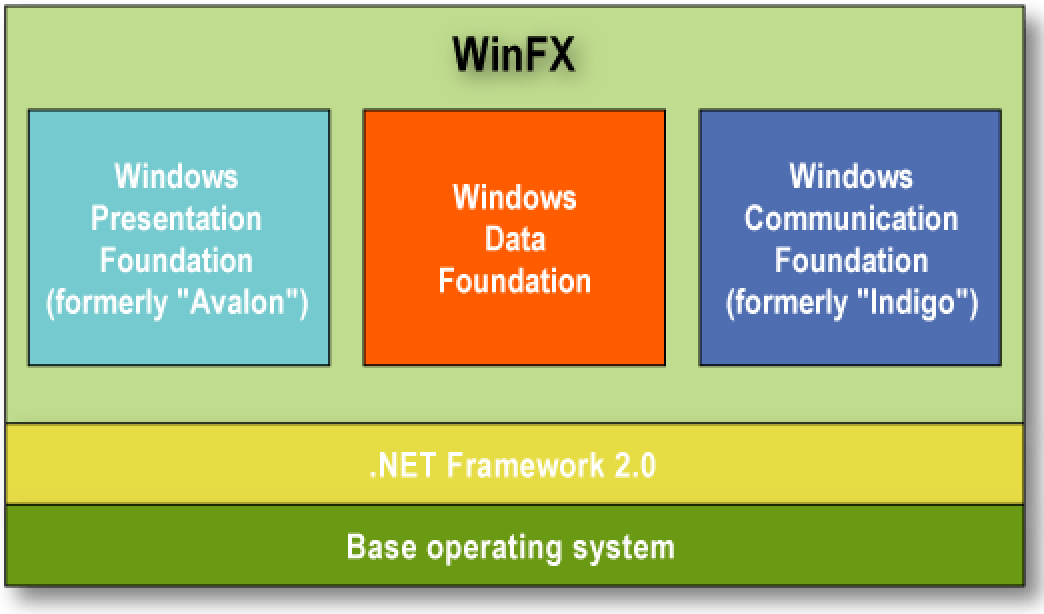
WinFX
Windows Presentation Foundation (formerly "Avalon")
Windows Data Foundation
Windows Communication Foundation (formerly "Indigo")
.NET Framework 2.0
Base operating system

Figure 2: *High-Level Architecture of Windows Vista Operating System*

Figure 2 obscures a great many moving parts, such as the Windows Workflow Foundation application programming interfaces (APIs) and developer components. Also, the WDF is not at the same level of completion as WPF and WCF, in part because it is dependent on Language Integrated Query (LINQ) and WinFS, which aren't as far along as WPF and WCF.

Not shown or renamed yet is WinFS, the relational file system that remains in early beta. With the goal of representing all sorts of digital objects or items as files and making them all accessible through the ActiveX Data Object for .NET (ADO.NET) API and other interfaces, WinFS is an extremely ambitious piece of technology that keeps being delayed; its client component will not ship with Windows Vista, nor will its server component ship with “Longhorn” Server.

What about the server? Windows Server 2003 R2 is a new release, not a service pack, but while it adds many features, it does not fundamentally re-architect the preceding server. The release still code-named Windows Server “Longhorn” will, on the other hand, incorporate major changes; WinFX will bolt onto the base server OS for application server use, but Microsoft will also release the “Server Core,” a headless domain controller without the web browser bits, web server bits, or (hopefully) much other functionality that is superfluous or dangerous from a security perspective where so much risk aggregates. Microsoft deserves considerable credit for providing simplified server packaging.

There will also be numerous enhancements to Active Directory, certificate services, federation services, rights management services, and identity integration services. The resulting manageability and control functionality will be impressive in many respects, but the continued emphasis on tight integration runs counter to the principle of loose coupling in modular service-oriented architectures (SOAs), and this may create inflexibility for some deployments.

For another Burton Group perspective on Vista, WinFX, and other platform subjects, see the *Application Platform Strategies* TeleBriefing, "Revisiting Microsoft's Platform/Tool/Application Strategies: PDC 2005 News and Updates."

Windows Vista and the Enterprise

The impact of Windows Vista and Server "Longhorn" will be measured not only by their ability to meet release dates and deliver promised features, but also by the pace of uptake in enterprise customer environments. Enterprises are usually cautious about major operating system changes, waiting for one, or even two, service packs to be released before commencing deployment. But to the extent it can accelerate deployment, Microsoft will strengthen the virtuous cycle of third-party support and market momentum for Windows Vista and Server "Longhorn."

Microsoft's arguments for accelerated deployment of their new releases include:

- **Productivity:** The new operating system clearly provides many features—such as quick search, virtual folders, helper applications, and enhanced APIs for yet more independent software vendor (ISV)-provided applications—to improve user productivity.
- **Enabling distributed workforces:** Windows Vista features that support mobile and distributed workforces include peer-to-peer collaboration tools, such as Meeting Space, and data protection via drive encryption.
- **Manageability:** Enhancements for system installation image management and other features, including Group Policy enhancements, will make enterprise deployment and management easier and more cost-effective.
- **Compatibility:** Windows Vista retains compatibility to Win32 APIs and Microsoft has promised developers that many applications written for Windows Vista will run relatively gracefully on Windows XP. Most, but not all, of the Windows presentation and communication foundations will be made available on Windows XP and Server 2003. But WCF will include more transaction management-related features on Vista, and WPF will exploit new hardware optimization services available only on Vista. Still, the "backported" versions will be quite satisfactory for most developers, at least in the near term.
- **Security:** A variety of security improvements could mean that deploying Windows Vista and the new server releases will reduce risks.

During one interview, a Microsoft representative said that Windows Vista deployment may bring about a 25% improvement in total cost of ownership (TCO) for personal computers (PCs). Digging deeper, however, the real issue is getting to a well-managed desktop environment with standard desktop images, automated software distribution, centralized policy management, and the like. Without effective desktop management, the same representative estimates TCO can run a whopping $5,000 per desktop per year; with it, TCO drops dramatically. Today, fewer than 25% of organizations with 500 or more computers have a well-managed desktop environment. Although Burton Group has not conducted quantitative studies that might corroborate these estimates, they seem to be in the ballpark. Thus, the first order of business for enterprises without a managed desktop environment is putting the house in order. Moving to a new client OS at the same time may or may not facilitate that goal.

Security in the Balance—A Key Success Factor

Almost two years ago now, Burton Group wrote the *Security and Risk Management Strategies* report, "Windows Server 2003 Security: Making Progress, But Serious Concerns Remain." That title speaks for itself. Today's $64,000 question is: With Windows Vista, has Microsoft resolved those serious concerns? Because Vista remains unfinished and many details of the Server "Longhorn" release are still missing, it would be foolish to answer categorically. But enough information has come out to clearly identify positive and negative factors.

On the plus side, Microsoft has done the following:

- **Rebuilt and reengineered the code:** The Windows Vista client code was rebuilt on the relatively more robust Windows Server 2003 code base. Development and security teams also created, refined, and followed a Security Development Lifecycle (SDL) that should improve the quality of the released product.
- **Improved privilege management and style of use:** Windows Vista incorporates a set of changes referred to as User Account Control that reduce the requirement for users and applications to use the system in administrator mode. This corresponds to the extremely important principle of least privilege. Even if

successfully attacked, a user process or a service running in standard user mode is less likely to do serious damage than a process running in administrator mode. See "The Details" section of this overview formore information on User Account Control.

- **Service hardening, device drivers, and reliability:** Service hardening does for Windows Vista OS and application tasks what User Account Control does for humans. Services generally run with lower privileges and additional access controls. Also, some device drivers no longer need to run in the operating system kernel, lessening the chance that third-party code could compromise a system. For example, Microsoft says that 30% of system crashes result from display driver faults in versions prior to Windows Vista; these occur because video capabilities are given privileged execution status. To remedy this, Vista will isolate the video subsystem. A Group Policy setting can also be configured to prevent installation of certain types of devices; an enterprise could use this setting to make a client system more stable or to prevent insertion of a universal serial bus (USB) storage device, for example.
- **Browser security improvements:** The Internet Explorer 7.0 (IE7) browser will operate in two modes—"protected" and "elevated." IE7 will run in protected mode by default, creating a sandbox such that malware may not be able to affect the computer as a whole, tamper with other user accounts, or even permanently affect the user account in which the browser is running. If a user needs higher-level permissions to complete a specific function, elevated mode will remove those security limitations. Both modes will provide anti-phishing features, eliminate silent ActiveX install, and warn the user of unsafe settings.
- **Authentication enhancements:** InfoCards will provide users with a protected visualization of personas and credentials for use in multiple environments. Although enterprises are unlikely to adopt InfoCard as a workforce solution, InfoCards may proliferate in the consumer environment, bringing reduced sign-on and increased use of strong credentials in its wake. Meanwhile, enhancements to Winlogon, smart card interfaces, and a Cryptography Next Generation (CNG) API will make it easier for developers to field multifactor authentication solutions. Microsoft will complement these capabilities with server-side enhancements such as federated identity and certificate life cycle management support.
- **Auditing enhancements:** Vista will provide new event logging infrastructure with stronger filtering and the ability to initiate tasks if certain kinds of events occur. The system can also forward events to other machines with remote audit trails as well.
- **Hardware integrity and process isolation:** Windows Vista will support the Trusted Platform Module (TPM) 1.2 specification to improve bootstrap boot cycle assurance and provide full-volume encryption. With that, the risk of a lost or stolen laptop may be reduced. However, the TPM will not be used for any Windows public key infrastructure (PKI) operations. Other enhancements protect the user desktop process from malicious services and increase the surety of process isolation. For more information on TPM, see the *Security and Risk Management Strategies* overview, "Next-Generation Trustworthy Computing: Reality Falls Short of Potential ."
- **Server code minimization:** As noted earlier, the Server Core and other role-specific packaging of Windows "Longhorn" Server will make it easier for customers to deploy hardened server solutions with reduced attack space, especially in the all-powerful domain controller role.
- **Other enhancements:** Microsoft is starting to lay the road map for content control solutions with recent announcements or beta releases of anti-virus, anti-spyware, anti-spam, and consumer PC health-monitoring solutions. Although most of these will be premium products, the basic OS will provide a Malicious Software Removal Tool (MSRT) and the Windows Defender anti-spyware functionality to remove as much malware as possible from an existing machine when Windows Vista is installed. The Windows personal firewall will also be enhanced to give the information technology (IT) administrator the ability to set policy to block certain applications (such as instant messaging [IM] or peer-to-peer) from communicating on the network, but this is not a defense against malware that tries to embed itself in an application.

On the minus side:

- **Size and complexity:** The client OS comprises something north of 60 million lines of code, and balloons to over 100 million when tightly integrated Office features are installed. Moreover, considerable complexity results from the intricate processing required to provide least-privilege mode operations while remaining backward-compatible to as many applications as possible—as well as the complexity arising from continuing to support ActiveX in the browser while attempting to limit its potential for malicious effects. Microsoft is making many efforts to balance security and usability; some of these allow customers to turn off undesired features. But Murphy's Law applies: If the undesired feature is there, it might be exploited.

- **ActiveX remains:** Whereas Java and .NET applications can run in a protected browser sandbox or other restricted contexts, ActiveX installs code in the Internet Explorer browser and runs it with full code privileges on the machine. Most spyware and many worms have exploited ActiveX to attack PC systems. Why not get rid of ActiveX, or phase it out? Microsoft argues that a substantial developer community has formed around ActiveX and it would be detrimental to preclude ActiveX on Windows Vista. Moreover, ActiveX is turned off by default, and enterprises can choose to block ActiveX themselves through Group Policy (for either the Intranet or Internet Zones as defined by Windows security) and, in any case, improved browser protections will reduce the risks associated with ActiveX. But when enabled, ActiveX's risks to users are analogous to those associated with e-mail attachments.
- **No code minimization on the client:** Microsoft has provided a “Server Core” packaging that strips out all functionality except what is necessary to provide a domain controller; however, no “Client Core” packaging has been described for higher-surety workstation uses. While Microsoft is delivering a slimmed down “Remote Desktop” version of Windows XP for enterprise use in online mode only, the company argues that with Windows Vista it cannot afford to break the value proposition of continuity and standardization—600 million clients running the Win32 APIs available to the same applications.
- **Popular target for attackers:** By virtue of being the most widely used OS, Windows will remain the most popular target for hackers. There is, of course, relatively little Microsoft can do about that problem.

Bottom Line for OS Security

On balance, Burton Group concludes Windows Vista and Server “Longhorn” will be more secure than any preceding Microsoft operating system. The arms race between attackers and software vendors will continue, but Windows Vista will raise the bar.

Once in the field, Windows Vista will also benefit from generally improved security infrastructure and practices; Microsoft has done much to improve industry defenses through a substantial investment in prescriptive guidance, emergency response processes, cooperation with law enforcement, patch management update systems, and OS security enhancement through service packs. Microsoft has also invested in education, providing a great deal of documented prescriptive guidance for customers. The enhanced Microsoft OS and the improved industry defenses will reinforce Microsoft customers' ability to protect the users and information assets reposed in Windows.

Readers have also asked Burton Group whether “serious concerns” remain with Windows Server 2003 itself. This, too, requires a complicated answer. In one sense, Windows Server 2003 is still the same server that it was when we wrote the above-referenced report and the same concerns exist. In another sense, however, the security climate has distinctly improved from the 2003 and 2004 time frame when worms ravaged enterprise networks and actually shut down rail services, banks, and factories in isolated cases. Microsoft's own efforts deserve much of the credit for this improvement. Increased customer deployment of firewalls and other third-party security tools for defense in depth have also done much to rein in the worms. But at the same time, attackers have shifted their focus to exploit new weaknesses in Windows, Internet Explorer, and the users and applications themselves. Microsoft has helped its customers win some battles, but the war goes on.

In response to other questions, Burton Group will not compare future versions of Windows, Linux, UNIX, Macintosh, or Firefox in this document as we feel such a comparison would at this point be founded on forward-looking statements from the parties involved, not provable security. There are advantages and disadvantages on each side of the platform security debate. In general, some non-Microsoft operating systems and browsers should continue to benefit from relatively less attacker attention and exhibit somewhat less complexity than Windows. However, security by obscurity (and simplicity) would not be the only rationale for platform selection even if security were the only decision factor. Windows continues to enjoy more support from third-party security vendors. Also, Active Directory, Group Policy, Certificate Services, and other Microsoft features provide advanced security functionality that is not generally integrated into most competitive OS platform environments.

New Products for Content Control

Through the Client Protection Technologies announced in October 2005, Microsoft will for the first time provide a host-based content control suite to mitigate malware, and Exchange will provide anti-virus and anti-spam capabilities. Initially, some of these premium products will lag best-of-breed content control vendor offerings, but over time, Microsoft will improve the products and provide increasing value through its ability to integrate features with the OS and by leveraging a global malware community-monitoring system, which will collect data from millions of Windows systems.

Although Client Protection Technologies will obviously compete with third-party security vendors, Microsoft seems to appreciate the continuing value that security vendors provide customers. For example, the Antigen product for Exchange, SharePoint, and Instant Messaging provides and integrates up to eight leading scan engine technologies from other anti-virus vendors. Microsoft is also sponsoring a program called the Microsoft Security Alliance. Through this alliance, Microsoft will cooperate with vendors seeking to provide protections in a way that is better integrated with the Windows platform.

As will be described in the upcoming *Security and Risk Management Strategies* overviews, "VantagePoint 2006–2007: Information Security Trends" and "Root Document: Making Business Sense of Information Age Security," attackers will evolve, continuing to use increasingly sophisticated variations on spyware and phishing themes. Signature-based content filtering will become even less effective than it is today, necessitating identity-based and behavior-based preventive approaches that will have to go toe-to-toe, round after round, with exploit coders, script kiddies, and organized cyber-criminals. Both Microsoft and the third-party security vendors must deploy next-generation behavioral solutions to malware. Faced with competition from Microsoft, the third-party security market will evolve, suffer setbacks, but generally continue to find viable and important security niches. Microsoft's advantage lies in the integration it can bring across broad product lines, but third parties will continue to be more nimble and more resistant to common mode failures.

Longer-Term Outlook

While much improved from previous releases, Windows Vista and Server "Longhorn" will remain large, flexible and complex general purpose operating systems. Content control protections will still need be added to the out of the box installation in almost all cases for protection against continually changing viruses, worms, and other malware. Customers should still take additional hardening, covering, or compensating measures to raise surety1 when deploying these high-usability systems in environments characterized by medium or high risk.1 (See the *Security and Risk Management Strategies* overview,"Concepts and Definitions," for formal definitions of surety, risk, and other terms.)

There are hard tradeoffs between usability and security. Murphy's Law, exploit coders, and high-tech social engineers take no prisoners; high surety comes only with a code-minimized, locked-down system, or a very isolated system. On the other hand, it takes a power user's workstation connected to the Internet and loaded with features to deliver the ultimate in usability. Security isn't everything, and the world clearly needs general purpose operating systems.

Must the tradeoffs between usability and security be so harsh—always? Microsoft and other vendors are working to improve matters through OS-level TPM and virtual machine (VM) support. Someday, an OS may run a hardware kernel that switches control and passes information only in a trusted manner between multiple, locked-down, task-oriented VMs, workplace VMs for power users, and disposable VMs for the freewheeling gamer/surfer—all on the same PC.

Achieving such an exquisite balance of control and usability on a single system in a way that meaningfully increases surety—and is foolproof and intuitive for the lay user—will likely take two or three iterations of Microsoft's planned hypervisor or similar technologies. The first version of the hypervisor will not ship until sometime after Windows Server "Longhorn" though other virtualization solutions from VMware, Microsoft, and other vendors will be available in the meantime. Microsoft will continue to ship its Virtual Server and promote VM image standards and other capabilities. One Microsoft representative suggested another approach to security and virtualization, wherein application vendors could ship applications as VMs intended for server-based deployment with user access through terminal services. Still other solutions from other vendors may also attempt to cross the hitherto impassable divide between extremely hard to use but trusted systems, and easy to use but vulnerable general purpose systems.

Recommendations

Windows Vista and “Longhorn” Server increase both usability and surety, raising the bar considerably above previous OS releases. Be glad, but be realistic—yet more insecure applications, user errors, persistent attackers, and an increasingly potent online criminal element will raise the threat level as well. Risk remains the only certainty. In that light:

- Supplement technical safeguards with strong process controls such as change management, testing, and awareness programs appropriate to the risk level.1
- Maintain strong covering measures through a layered defense that resists common mode failures by leveraging multiple types of controls from multiple vendors.
- Cease, desist, block, and disable ActiveX. Conduct most development in appropriate script languages, Java, and .NET instead.
- Where possible, deploy Windows desktops and even laptops in standard user mode. If administrator privileges must still be granted to users, ensure that Windows applications take full advantage of opportunities in Windows Vista and Server “Longhorn” for least-privilege mode operations as described in the “User Account Control” and “Windows Service Hardening” sections of this overview. Train internal developers on these good practices, and institute appropriate purchasing and vendor management requirements.
- Consider thin-client solutions such as Citrix, X terminals, and yet another planned Microsoft OS called Windows Fundamentals for Legacy PCs (WinFLP, formerly code-named “Eiger”).
- Consider Windows Remote Desktop for work functions that are always online.

After evaluating and testing carefully to prove feature and robustness claims, and obtaining a positive risk assessment:

- Replace all Windows domain controllers with Server Core as soon as possible, especially when domain controllers cannot just be removed from remote sites.
- Achieve a managed desktop environment and schedule migration of Windows clients and servers to Windows Vista and “Longhorn” Server based on business considerations (security is a positive for migration).
- Consider deploying the TPM-enabled BitLocker Drive Encryption and full-volume encryption features, but only with enterprise management oversight and a data recovery process in place.

After evaluating and comparing against competitive products, testing carefully to prove feature and robustness claims, and obtaining a positive risk assessment:

- Consider Microsoft's certificate services and related components to increase surety of authentication, integrity, and confidentiality.
- Consider using Active Directory Federation Services (ADFS) internally to the enterprise for cross-platform single sign-on and to replace interforest trust relationships in certain cases.
- If ADFS proves usable and popular in the small to mid-size business (SMB) environment, consider encouraging and enabling (but not requiring) your SMB partners to use it.
- If third-party InfoCard site support spreads, consider using InfoCard as a means of user-centric federation.
- Consider using Microsoft's integrated content controls, in combination with third-party content control vendors, as the threat evolves.

The Details

The following sections contain details on these topics:

- User Account Control
- Windows Service Hardening
- Windows Server 2003 R2 Changes
- Windows Server “Longhorn” Plans
- InfoCard
- Internet Explorer 7.0 (IE7)
- Windows Communication Foundation (WCF)
- BitLocker Drive Encryption and the Trusted Platform Module (TPM)
- Microsoft Steps into Content Control
- A Thin-Client Option from Microsoft

User Account Control

Windows Vista and Server “Longhorn” will essentially be variations on the same operating system (OS) code base, and of all the security enhancements to that code base, User Account Control will probably make the greatest impact. When running in administrator mode, applications have enhanced opportunities to subvert the system. However, User Account Control reduces the requirement for applications to run in administrator mode. This area of functionality is complex but very promising because it imposes and encourages changes to the “single user” style of use that has been a bane to Windows security over the years.

Historically, because of Windows' consumer orientation, most applications required full administrator privileges to install or—sometimes—to even run. But Windows Vista will provide a number of “secure by default” techniques to make imposing the principle of least privilege less painful. These will include just-in-time privilege elevation, administrator approval mode, and virtualization of privileged write attempts by legacy applications.

- **Just-in-time privilege elevation:** Users logged in as standard users who run setup applications requiring administrator privileges will be prompted to provide administrator credentials without having to log off. The setup succeeds.
- **Administrator approval mode:** Users logged in as administrators will have their privileges automatically lowered and will be prompted before doing anything that would require administrator privileges. However, administrators will not have to log in again. This might prevent malicious code on a website from silently installing. Administrator approval mode can be enabled or disabled through a system setting.
- **Virtualization of privileged write attempts:** If a legacy application running in standard user mode tries to write information to a protected area of the Windows registry, or to write files to “program files” or other system folders, Windows Vista and Server “Longhorn” will create a virtual store and redirect the writes to a per-user location. To the program, the write to “program files” appears to succeed. (The downside to this is that your kids running different user accounts will each think he or she has the high score for *Doom*. This may be good for their self-esteem, but has weird results in other applications.)

As just discussed, the OS will try to guess when applications legitimately require elevated privileges, but for the best results, application developers should plan to write per-user mode applications and avoid using administrator privilege when it isn't required. Developers should identify their privilege requirements in the “application manifest” and interact with users through a “shield graphic” so that users can request privilege elevation when it is needed. The just-released Visual Studio 2005 development environment will include a “permission calculator” and other features to help developers manage their privilege requirements. All of this represents a major culture shift and retraining effort that will take considerable time to reach fruition. For more information on these and other security features, see Microsoft's site for Windows Vista security and protection.

Windows Service Hardening

Windows Service Hardening may restrict Windows operating system tasks (called services) from performing abnormal or dangerous activities in the file system, registry, network, or other resources that could be exploited by malware. For example, the remote procedure call (RPC) service could be restricted from replacing system files or modifying the registry.

Windows Vista will reduce exploit opportunities by limiting the number of services that are "always on" by default, and by reducing the number of services that run in the LocalSystem account, where any breach could lead to unbounded damage to the local machine—including disk formatting, data or privilege alteration, or malware installation.

Windows Service Hardening will introduce a per-service security identifier (SID) to enable per-service identity for use with Windows access control. Services will be able to apply explicit access control lists (ACLs) to resources that are private to the service, which prevents other services or users from accessing these resources.

- Stripping of unnecessary Windows privileges on a per-service basis—for example, the ability to do debugging
- Application of a write-restricted token to the service process; this can be used in cases where the set of objects written to by the service is bounded and can be configured (write attempts to resources which do not explicitly grant the service SID access will fail)
- Assignment of services to network firewall policy, which prevents network access outside the normal bounds of the service program; the firewall policy will be linked directly to per-service SID

Windows Service Hardening will provide an additional layer of protection for services based on the security principle of defense in depth. Windows Service Hardening will not be able to prevent a vulnerable service from being compromised, but it may limit how much damage an attacker can do. Windows Service Hardening features should also be employed by third-party developers.

Windows Server 2003 R2 Changes

The Windows Server 2003 R2 release is planned for the end of 2005. Fully described in a reviewer's guide, it will include enhancements for simplified branch office server management, simplified identity and access management, efficient storage management, and additional features. The features that are most interesting from a security perspective include:

- **Active Directory Federation Services (ADFS):** ADFS builds on the previously released "protocol transition" application programming interfaces (APIs) to allow a web user session to map into an account that is Active Directory enabled with all of the group memberships and other attributes or privileges associated with that account in the Windows OS authorization scheme. Since ADFS communicates over Hypertext Transfer Protocol (HTTP) and does not require manual symmetric key management and distribution, federation is much easier and safer to deploy than interforest trusts in the Microsoft to Microsoft cross-domain environments. Security Assertion Markup Language (SAML) support will make ADFS interoperable with non-Microsoft software, but vendors will have to also implement the WS-Federation Passive Profile features. Fortunately, these additions do not seem to be very onerous for vendors. (For more information on federated identity interoperability, see the *Identity and Privacy Strategies* Methodologies and Best Practices document, " Multiprotocol Federation Interoperability Demonstration.")
- **Active Directory Application Mode (ADAM) in the box:** ADAM enables customers to deploy a Lightweight Directory Access Protocol (LDAP) server without deploying an entire Windows domain or affecting an existing domain controller. This is a handy feature for developers and for application-specific directory needs. Formerly, ADAM was only available as a download.
- **Active Directory as Network Information Service(NIS) master, Services for UNIX, and password synchronization with UNIX:** These products offer improved functionality for customers that wish to migrate from UNIX to Windows. For long-term coexistence, however, customers could consider other Windows-UNIX interoperability solutions from vendors such as Vintela, Quest Software, Symantec/BindView, and so forth.

For more information on Active Directory, ADFS, and ADAM, see the *Identity and Privacy Strategies* report, " Microsoft Windows Server 2003 Active Directory Revisited."

Windows Server “Longhorn” Plans

Slated for sometime in 2007 and now just entering its first beta release, Microsoft plans for Windows Server “Longhorn” to provide a number of security and manageability features:

- **Overall improvements:** This bullet is short but very significant. Because the client and server are essentially the same OS exposed in two different ways, the User Account Control, full-volume encryption, BitLocker Drive Encryption, and other security improvements provided in Windows Vista will also be available on the server, along with the WinFX stack. The server has also benefited from the engineering processes of the Security Development Lifecycle and the Common Engineering Criteria.
- **Server Core (modular packaging and code minimization):** For the first time, Microsoft will provide specialized server deployment packages for security purposes. The Server Core package will be a domain controller in a box, without all potential vulnerabilities of a general-purpose OS because the code for browser, ActiveX, and other functions will simply not be there. In fact, Server Core does not even have a graphical user interface (GUI), but it does comprise networking, Active Directory, and remote management capabilities. Server Core will be especially useful for branch office or remote site domain controller deployments, but may also be used in larger data centers as well.
- **Server Core Plus and role-specific server installation:** Server Core Plus will build on the Server Core base to become a more richly appointed application server including the Windows Shell, .NET Framework 2.0, tools, and Microsoft Management Console (MMC) with numerous other applications. In addition, the server will be configurable for specific roles at install time. Also, when an information technology (IT) administrator installs a new server role, the system will dynamically check for security updates for that particular role and make sure that the latest vulnerabilities are patched during installation.
- **Network Access Protection (NAP)**: The NAP functionality for endpoint admission control will be provided by the combination of Windows Server “Longhorn,” and a complementary client release such as Windows Vista. When a client machine connects to the network, locally or remotely, Windows Server “Longhorn” can verify that the client has the proper security patches, virus signatures, or system firewall and redirect the device to a quarantine network for limited access or remediation. For more information on NAP, see the *Security and Risk Management Strategies* report, “Enforcing Endpoint Security Policy Compliance: Early Products and Progress Toward a Standard.”
- **Internet Information Server (IIS) 7.0 modularization:** Whereas one has to be an administrator to use IIS 6.0 (which comprises a single Data Link Layer [DLL] with a private interface exposing the Internet Server API [ISAPI]), IIS 7.0 will leverage Active Server Pages for .NET (ASP.NET) configuration files that can be controlled by lower-privilege users and it will expose a public API to managed-code applications. Most importantly, IIS 7.0 can be configured to load in a modular manner so as to minimize bloat of unwanted features that could create or expose vulnerabilities. Thus, only the necessary modules reside in memory or need to be patched.
- **Management improvements:** MMC 3.0 will allow developers to build management applications using managed code. Terminal Server will be able to remote any application or management console on any machine. A new System Definition Model (SDM) demonstrated at the Professional Developers Conference (PDC) is planned to close the loop between operations and development by allowing developers to model how an application will be managed in deployment. Using code from partner Macrovision, Microsoft demonstrated the ability to visually set up monitoring and configure what type of events to trap and what data to log. In addition, Microsoft plans to provide an object-based command language called Monad that runs on .NET but reads Python scripts, Microsoft shell scripts, and so on.

Features that will *not* be provided in Windows Server “Longhorn” are virtualization in the OS (the hypervisor), the server components of WinFS, or management tools enabling virtual hard disks. These features are planned for a subsequent release, perhaps as a feature pack.

Active Directory

Microsoft is continuing to enhance Active Directory and to improve its integration with certificate services, federation services, rights management services, and identity integration services. The combination of these services will empower Active Directory customers, but it will also make individual services less modular. Customers will still be able to use Active Directory with third-party tools on top of it, but attempts to use the higher-layer Microsoft services will tend to create cascading requirements to implement an all-Microsoft solution. On the other hand, Microsoft's ongoing component integration efforts will make it easier to deploy capabilities like public key infrastructure (PKI) or Encrypting File System (EFS) in some cases.

Certificate Services

The Microsoft Certificate services have been adopted by a number of enterprises as a Certificate Authority (CA) function integrated with Active Directory and Windows servers. Apart from any other enhancements Microsoft may provide, security staff will likely appreciate the ability, with Windows Server “Longhorn,” to run a CA using the Server Core packaging, which hardens the CA server by stripping down the code base. Assurance of certificates and private key management on clients and servers supported by the CA will be improved by the Cryptography Next Generation (CNG) API, which ultimately replaces Cryptographic API (CAPI). The EFS will be enhanced by enabling key storage on a smart card.

In order to improve the overall manageability of the PKI environment, Microsoft also recently acquired certificate management vendor Alacris that offered one of the products that a number of enterprises had already been using to improve key recovery, key management, smart card management, and other necessities. See the *Identity and Privacy Strategies* report, “Public Key Infrastructure: Making Progress, But Many Challenges Remain,” and the Alacris website, for more information.

Federation Services

Windows Server “Longhorn” will inherit the ADFS functionality described above in the section on Windows Server 2003 R2. ADFS enhancements are possible or likely to address the following areas:

- Availability of ADFS and InfoCard features to Visual Studio developers through the WinFX programming model.
- Smoothing out the glitches and limitations that will likely appear when customers attempt to use Microsoft's features plethora with web-based federated login through ADFS rather than the normal Windows login.
- The Sun-Microsoft Web Single Sign-on (SSO) Interoperability Profile, which was developed to enable Liberty Alliance's Identity Federation Framework (ID-FF) users to employ SAML with account linking functionality. This functionality has previously been demonstrated by Sun and Microsoft, but is not planned until after Windows “Longhorn” Server.
- Burton Group and customers will continue to push Microsoft to provide direct interoperability with Organization for the Advancement of Structured Information Standards (OASIS) SAML browser profiles, rather than only exposing SAML through the WS-Federation Passive Profile. Microsoft has resisted making such changes in the past, but this often-pragmatic software vendor may eventually respond to customer requests. Directly supporting the OASIS SAML 2.0 browser profiles would enable a host of technical and security improvements associated with federation, single sign-on, and browser mechanics that numerous OASIS experts labored long and hard for more than a year to create and that should not be reinvented or ignored.

A feature that will *not* be provided in Windows Server “Longhorn” ADFS is the Security Token Service (STS) implementing all the features of the WS-Trust. Full STS is planned for a subsequent release, perhaps as a feature pack.

Rights Management Services (RMS)

Microsoft refers to RMS as an “information rights management” product to differentiate it from similar, but consumer-oriented, digital rights management (DRM) offerings. RMS enables users of Microsoft Office 2003 and later versions, or users of other RMS-enabled applications, to attach cryptographically enforced usage controls to various types of documents such as e-mails, spreadsheets, presentations, forms, or word processing documents. These rights, or controls, stay with the content even when the content has moved outside the originator's control or is being used offline. To access the controlled content, the recipient must first obtain a license from an RMS server, which has the ability to determine the recipient's identity and privileges from Active Directory.

RMS is and will continue to be a premium service of Windows and to be licensed via a Server Client Access License (CAL) model like Terminal Services. Beginning in Windows Server 2003 R2 and on into the Server “Longhorn,” RMS will be more tightly integrated with Active Directory and with ADFS to allow greater reach in cross-domain environments and other improvements.

Microsoft also plans to provide functionality in RMS based on an Extensible Markup Language (XML) Paper Specification (XPS) intended to compete with Adobe Acrobat. APIs in Windows Vista will allow developers to rights-enable XPS document packages. User documents could be created from applications, such as those in computer-aided design/computer-aided manufacturing (CAD/CAM), which allows rights enabling of anything that supports the package. Microsoft hopes that as third-party support grows, developers will see interoperability and compatibility benefits; for example, an RMS-enabled application might automatically work with an archiving package by way of the XPS package abstraction. From a user point of view, XPS documents can be created from any application and can then be rights protected with RMS via the XPS Viewer that will ship with Windows Vista.

Identity Integration Services

Microsoft provides identity integration services through Microsoft Identity Integration Server (MIIS) and the Identity Integration Feature Pack (IIFP), which is the version of MIIS shipping with connectors only for Active Directory and ADAM. MIIS has the goal of growing up to become a full meta-directory/provisioning hybrid, while IIFP seeks to provide automated OS-embedded synchronization capabilities that can be used by low-skill administrators. IIFP is licensed as part of Windows Server Enterprise Edition.

Planned enhancements to Microsoft's identity integration services include:

- Web-based self-service password reset
- Deeper integration with ADFS and Authorization Manager (AzMan) to enable rules-based entitlement management
- The ability to leverage Windows Workflow Foundation for provisioning tasks including the ability for web services to request entitlements
- Support for dynamic groups and computed attributes
- Compliance-oriented features, such as comprehensive auditing with data lineage and entitlements reporting
- Connectors to SAP, ACF/2, PeopleSoft, TopSecret, and AS/400 (appearing variously during late 2005 and 2006 for MIIS only)

Through all this, MIIS and IIFP will continue to leverage Structured Query Language (SQL) Server for their own storage needs. Burton Group also speculates that in the far future, Active Directory and IIFP synchronization capabilities may play an enabling role for WinFS navigation, synchronization, and other features, but we have no specific information on this.

InfoCard

InfoCard is a personal identity selector (or single sign-on utility) planned for Windows Vista with phishing resistance and credentials database functionality built in. InfoCards will appear in the user interface when the user invokes a control panel application or attempts to access a Uniform Resource Locator (URL), or resource, requiring authentication that is accessible through the credentials in one or more InfoCards. The user will also interact with InfoCards through a separate desktop interface that Microsoft says will reduce the risk of malicious code gaining access to credentials.

In some sense, the InfoCard functionality is analogous to the functionality found in a tool such as Roboform today. Roboform, for example, allows the user to save passwords for multiple websites, fill out web forms, and log in automatically. It is user friendly and relatively secure in its ability to generate and remember strong passwords, encrypt login data, and protect login data through a master password. It can also run off a portable universal serial bus (USB) memory stick. InfoCard will likely aspire to similar flexibility and user friendliness.

The difference between InfoCard and packages such as Roboform is that InfoCard can employ multiple types of authentication and credentials, not just passwords. Soft certificates, symmetric keys, assertions (claims), or attributes may be involved. InfoCard uses cryptographic keys to identify the user to a site and a site to a user; that is, a password is not passed to the relying party. This in itself improves the authentication assurance somewhat, but a second biometric or hardware token form factor will still be necessary to truly strengthen authentication.

InfoCard also offers some interesting possibilities to raise the bar for standards-based interoperability of multiple types of authentication and credentials. Users can generate self-asserted credentials, or domains and sites can issue credentials to users as InfoCards. However, the sites and domains will need to be programmed to work with InfoCard, and at this point Microsoft is mostly offering APIs rather than full-featured STS functionality which, as noted earlier, was deferred until the post-2007 time frame.

As the *Identity and Privacy Strategies* overview, "User-Centric Identity Management and the Enterprise: Why Empowering Users Is Good Business," describes in more detail, an InfoCard represents a relationship with an identity provider, or it can be self-issued (and editable) by the user. A card will contain metadata allowing applications to obtain a security token from an identity provider using WS-MetaExchange, WS-SecurityPolicy, and WS-Trust. The security token issued by the identity provider will be submitted to the relying party by the user. InfoCard-enabled services can be implemented to protect the user's privacy by not enabling identity providers to track user activity across different sites. Also, when the user consents to using an InfoCard for authentication, the software in the Windows Vista client does not send all the available attributes in an InfoCard—only those requested by the relying party are released with the user's consent.

Microsoft's ADFS and other federation offerings with SAML, WS-Trust, and other features will provide an initial base for InfoCard usage. Future versions of Microsoft's online properties will likely support InfoCard along with some early third-party site adoption. Although there are a number of competing user-centric identity alternatives, Microsoft's well architected, open approach and powerful position in the industry create the distinct possibility that InfoCard will become a very widely used framework for Internet identity.

IE7

IE7 tries to strike an intricate balance between the customers' need for flexible browsing and the need to secure the browser.

Older versions of Internet Explorer have been very vulnerable to ActiveX malware, spyware, and phishing exploits. ActiveX controls can expose dangerous functions and security bugs at any time, yet users have little control over the number of controls installed by default. Some improvements in safely processing URLs were made for the current Internet Explorer 6.0 combined with Windows XP Service Pack 2 (SP2), but IE7 contains many additional changes.

IE7 will contain new safeguards to deal with a number of threats including URL parsing attacks, domain spoofing, buffer overruns in Internet Explorer or helper processes, dangerous file launches and installations, logic errors in prompts, malicious scripts, naïve users lowering security settings, and content that overlays false URLs or false information onto the user's display. In general, IE7 addresses these attacks through personal data protection features, advanced malware protection, and by providing more user control over add-ons.

The "personal data protection" features will include unified URL parsing to resist encoding attacks by canonicalizing URLs following the recommendations of RFC 3986. Developers will also be able to use the Internationalized Uniform Resource Identifiers (IURI) object in URLMON to canonicalize URLs. These features will include the following anti-phishing capabilities:

- Dynamic Phishing Filter blocks users from navigating to known phishing sites and notifies users when viewing websites bearing suspicious characteristics of phishing behaviors (based on an online service that tracks known phishing sites)

- Dynamic Phishing Filter (green bar for sites with high assurance certificates, red bar for suspect sites)
- Address bar appears on every pop-up window
- Background tabs can't open windows
- Internationalized domain names (IDNs) must be in a language supported by the user's system
- Multiple languages can't be mixed in an IDN URL (these language enhancements help ensure that the URL that user *sees* is the URL that is being browsed)
- Improved user visualization and awareness of secure (Secure Sockets Layer [SSL]-protected) operation or lack thereof

The advanced malware protection feature includes the browser's default operation in “protected mode,” which will still allow users to download files or change browser settings but impose restrictions to prevent exploits from escalating privilege to embed malware on user systems. Writes to the user's profile will be automatically redirected to a portion of the Temporary Internet Files where they should not cause harm to the personal computer (PC) environment. Developers will be able to build applications to run in “protected mode,” if they are intended to handle untrusted data. Developers could also configure file/registry ACLs that are safe and needed to ”low.” These low-integrity applications could also be programmed to communicate with a broker process that conducts any medium- or high-integrity operations required for the application.

Advanced malware protection features will also limit the functionality of cross-site scripting attacks and scripts that redirect the browser to different sites. Partner code should also enforce secure domain access rules and be redirect-aware. But, as should be clear from much of the preceding discussion, much depends on developers following the numerous guidelines, training to write secure code, and using code-scanning tools with Visual Studio or other environments.

Users and administrators will have more control over browser add-ons. To maintain compatibility in IE7 upgrades, previously loaded controls are enabled by default, but any new controls must be explicitly enabled. New IE7 installations will enable a small set of popular controls commonly used by Internet websites, such as the Microsoft Network (MSN). The so-called ActiveX Opt-in feature allows users to enable or disable ActiveX controls as needed through the Information Bar and Add-on Manager. IT administrators will also have the ability to disable ActiveX by Group Policy, but only on a per-zone basis. One Microsoft representative insisted that the ability to enable ActiveX for Windows' so-called “Intranet Zone” but disable it for the “Internet Zone” was a significant benefit. However, Burton Group would only recommend this approach for fixed desktop systems that do not move into Internet cafes, public wireless local area networks (WLANs), or other areas where “Intranet Zones” are extremely unsafe.

Windows Communication Foundation (WCF)

WCF is Microsoft's unified programming model for building web service applications with managed code. It extends the .NET Framework to enable developers to build web services with security, reliability, and transactional features using some of the WS-* specifications described in the *Security and Risk Management Strategies* overview, “WS-*: A Composable Architecture for Web Services Security,” and the *Application Platform Strategies* report, “Web Services Security: A Plethora of Products.”

WCF interoperates with or replaces existing Microsoft distributed systems technologies, including Enterprise Services, System.Messaging, .NET Remoting, Active Server Methods (ASMX), and Web Services Enhancements (WSE). It provides opportunities for application messaging using various transports or channels including HTTP, Transmission Control Protocol (TCP), named pipes, and the Peer Channel as well as security support for WS-Security signatures, encryption, or authentication using SAML, Kerberos, X.509, and Username tokens. Applications built on WCF can tie in with Microsoft's InfoCard for federation and Microsoft's AzMan APIs for role-based access checks.

WCF enables developers to expose Windows Forms applications, ASP.NET applications, console applications, Windows services, and COM+ services as web services endpoints. Typically, a developer uses high-level APIs and data structures through Visual Studio that hide many communication details in configuration. Figure 3 provides Microsoft's diagram of the WCF architecture.

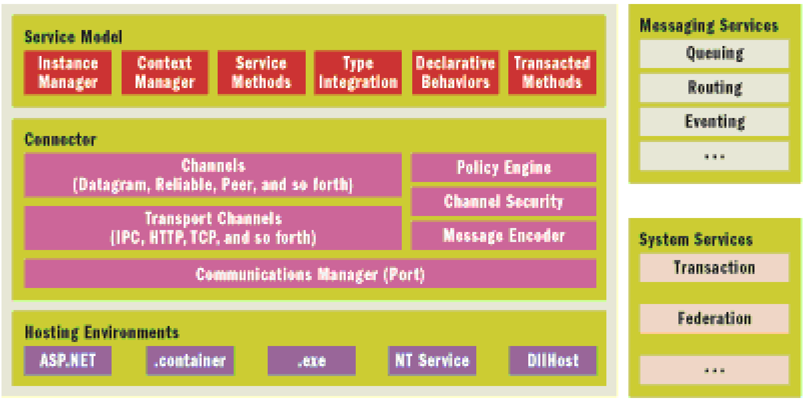

Figure 3: *WCF Architecture (Source: Microsoft)*

If key Windows services end up being exposed in a relatively pure and loosely coupled manner, WCF, with its open WS-* support, could foster widespread capability for applications to communicate in a device-independent and platform-independent manner. However, some applications may end up propagating legacy Component Object Model (COM) data structures and other Windows-specific dependencies over WCF's WS-* wrappers, thus making themselves less interoperable.

BitLocker Drive Encryption and the TPM

BitLocker Drive Encryption will add machine-level data protection, using a TPM 1.2 chip. Available only to enterprise users possessing machines with TPM 1.2 version install, BitLocker will also provide full-volume encryption of the hard drive, including Windows system files and the hibernation file using a symmetric encryption key. Access to the encrypted drive can be further protected by storing an encrypted password on a dongle, or requiring the user to enter a PIN. However, good management processes—and in some cases, tools—will be required to ensure that BitLocker Drive Encryption can be deployed with key recovery, PIN recovery, occasional boot sector patches, and other complications that will arise.

BitLocker Drive Encryption will also store measurements of core operating system files in a TPM chip. Every time the computer is started, Windows Vista will verify that the operating system files have not been modified in an offline attack scenario wherein an attacker boots an alternative operating system.

If OS files have been modified, or a disk drive is transferred to another system, Windows Vista will go into recovery mode, refuse to boot, and prompt the user to provide a recovery key for access to the boot volume.

BitLocker Drive Encryption is intended to protect the full machine against loss or compromise. EFS remains available to protect information on a multiuser machine. On Vista, the EFS key can be controlled using a smart card.

Microsoft Steps into Content Control

In the future, Microsoft will offer much more host-based content control than it provides today with the shipping Windows Firewall service. Plans to provide Microsoft Client Protection as an early 2006 limited beta were announced in October 2005. Microsoft Client Protection will combine anti-spyware tools based on the 2004 GIANT acquisition, anti-virus functionality based on the 2003 GeCAD Software acquisition, and centralized management for enterprise environments. These protection technologies will be backed by a global malware-research system that will sift through volumes of data submitted through the community and collected at Microsoft to help discover new threats faster. For more information on Microsoft's product and the anti-spyware market, see the *Security and Risk Management Strategies* report, "Enterprise Strategies for Defending Against Spyware."

Microsoft Client Protection will provide a centralized console for distribution of signatures and security reports throughout the enterprise. It will also be optimized for use with Active Directory and Windows Server Updates Services for distribution of client configuration and signature updates. Microsoft says the solution will be flexible enough to integrate with other software distribution systems that customers have in place.

Like the Windows OneCare beta with security, performance, and backup features that Microsoft now offers consumers and small businesses, the Microsoft Client Protection will be sold by subscription per user or per device on an annual basis through Microsoft's existing sales channels. The exact pricing or price range is unknown at this time, but the offering will likely undercut existing content control vendors such as McAfee, Symantec, Trend Micro, F-Secure, and others.

Microsoft also plans to release Microsoft Antigen anti-virus and anti-spam security software for Microsoft Exchange, SharePoint, and Live Communications Server based on the technology from recently acquired Sybari Software. Microsoft Antigen will leverage Microsoft's same anti-virus scan engine (originally GeCAD), but will also allow customers to plug in up to eight engines from other anti-virus vendors. The product will likely be provided as a premium offering, but Microsoft says that existing Sybari customers will be able to use the Microsoft anti-virus scan engine at no additional charge throughout the length of their contracts. Antigen is scheduled to be available in beta to customers in the first half of 2006. For more information on Microsoft Antigen, client protection, and other initiatives, see Microsoft's Security technology investments white paper.

In addition to Sybari, Microsoft recently acquired FrontBridge Technologies, which offers a hosted service for message security. Through FrontBridge Technologies, Microsoft provides customers a hosted option to scan and filter all e-mail traffic before it reaches their corporate network and internal messaging servers.

The Windows Defender anti-spyware tool and a Malicious Software Removal Tool (MSRT) will be provided to Vista clients at no charge.

A Thin-Client Option from Microsoft

Windows Fundamentals for Legacy PCs (WinFLP) is designed for customers who want to improve the security and manageability of older PCs. Built using the Windows Embedded Toolkit for Windows XP SP2, WinFLP is designed to run as a remote desktop client, but it will run local browsers, media players, instant messaging, document viewers, .NET framework, security applications, Windows Update, and other components. All other applications, including Microsoft Office, are not allowed by license, and must be run on the server. When employed with Windows Disk Protection technologies developed for the Microsoft Shared Computer Toolkit, WinFLP on reboot can wipe out all changes made since the previous boot. WinFLP will be available with Microsoft Software Assurance in spring 2006.

Conclusion

Windows Server 2003 R2, Windows Vista, and Windows Server “Longhorn”—coupled with Microsoft's industry-level security initiatives, greater emphasis on secure development practices, and planned forays into content control—will bring many security enhancements forward over the next two years. None of these changes guarantees higher assurance in all cases, but in combination they do make the overall security picture for Microsoft's enterprise customers appear much more promising than it has been in recent years.

Notes

[1] Burton Group. *Security and Risk Management Strategies* "Concepts and Definitions." 17 Jan 2005. http://www.burtongroup.com/content/doc.aspx?cid=644

Author Bio

DanBlum

Senior Vice President and Group Research Director

Emphasis: Security architecture, technology and products; identity management; federated identity management; directory services; secure e-mail
Background: Co-founder and principal of Rapport Communication, which merged with Burton Group in May 1998.

Primary Distinctions: Internationally recognized expert in the areas of security, directory services, federated identity and electronic messaging. Authored or co-authored over 50 vendor-neutral research reports, technical positions, and methodologies/best practices within technology focus areas. Consults for many Global 1000 companies on key strategic architecture and technology decisions. Served on International Standards Organization (ISO) and National Institutes of Standards (NIST) committees. Columnist for Network World. Co-author of "The E-mail Frontier," published by Addison-Wesley, 1994 and author of "Understanding Microsoft Active Directory Services," published by Microsoft Press, 2000. Speaks at prominent industry conferences including Catalyst, I4, Networld+Interop, RSA Conference, Digital ID World, Information Security Decisions, and many others.